UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
SAN ANTONIO

MELODY JOY CANTU AND DR. RODRIGO CANTU,

Plaintiffs,

v.

DR. SANDRA GUERRA and DIGITAL FORENSICS CORPORATION, LLC,

Defendants.

5:20-CV-0746 JKP – HJB

PLAINTIFFS' OPPOSITION TO DEFENDANT DR. GUERRA'S MOTION FOR SUMMARY JUDGMENT

Table of Contents

Plaintiffs Melody Joy Cantu and Dr. Rodrigo Cantu file this opposition in response to Defendant Dr. Sandra Guerra's ("Dr. Guerra") Motion for Summary Judgment. For the reasons stated below, this Court should deny Defendant's motion in its entirety.

Background

In their Amended Complaint, Plaintiffs assert claims against Defendants under the Federal Computer Fraud and Abuse Act, Texas's statutes covering unauthorized access to computers, as well as the Texas state tort of malicious prosecution.[1] Defendants jointly conspired to engage in the malicious prosecution of Defendant Melody Joy Cantu as well as the stalking and harassment of both Plaintiffs through a campaign of hacking, phishing, and surveillance in violation of federal and Texas law.[2]

The discovery shows that Defendant Dr. Sandra Guerra hired Defendant DFC to hack, investigate and surveil Plaintiffs.[3] As part of this conspiracy, DFC produced a "Phase I" report

---

[1] (1) Unauthorized Access to a Protected Computer 18 U.S.C. 1030(a)(2)(c); (2) Unauthorized Damage to a Protected Computer 18 U.S.C. 1030(a)(5)(A); (3) Unauthorized Access to a Protected Computer Recklessly Causing Damage 18 U.S.C. 1030(a)(5)(B); (4) Unauthorized Access to a Protected Computer Causing Damage And Loss 18 U.S.C. 1030(a)(5)(C); (5) Conspiracy to Commit Unauthorized Access to a Protected Computer 18 U.S.C. 1030(a)(2)(c) & 1030(b); (6) Conspiracy To Commit Unauthorized Damage to a Protected Computer 18 U.S.C. 1030(a)(5)(A) & 1030(b); (7) Conspiracy To Commit Reckless Damage to a Protected Computer 18 U.S.C. 1030(a)(5)(B) & 1030(b); (8) Conspiracy to Commit Unauthorized Access to a Protected Computer Causing Damage And Loss 18 U.S.C. 1030(a)(5)(C) & 1030(b); (9) Knowingly Accessing Without Effective Consent a Computer, Computer Network, Or Computer System Tex. Civ. Prac. & Rem. Code § 143.001 & Texas Penal Code § 33.02(a); (10) Knowingly Accessing a Computer, Computer Network, or Computer System With The Intent to Defraud, or Harm Another or Alter, Damage, or Delete Property Without Effective Consent Tex. Civ. Prac. & Rem. Code § 143.001 & Texas Penal Code § 33.02(b-1); (11) Electronic Access Interference Tex. Civ. Prac. & Rem. Code § 143.001 & Texas Penal Code § 33.022; and (13) Malicious Prosecution.

[2] *See* Dkt. 6, Am. Compl.

[3] *See e.g.* BATES#: D 000060-61 (Aff. of Dr. Guerra stating she has retained DFC (attached as Ex. A)).

for Defendant Dr. Guerra.[4] The Phase I report contained a sample affidavit written by DFC for use by Dr. Guerra to submit as part of a police report. DFC required the filing of the police report in order to do further work for Defendant and generate a "Phase II" report. Defendant Dr. Guerra admitted at depositions that the affidavit she submitted to the police was substantially written by DFC and not her.[5] Moreover, the Phase I report and communications between DFC and Dr. Guerra reveal that DFC created tracking URLs deployed by Dr. Guerra against Plaintiffs.[6]

The record establishes that Dr. Guerra and DFC phished Plaintiffs multiple times via text and email. DFC intentionally employed phishing links to gain access to Plaintiffs' networks.[7] During the same time period, Plaintiffs discovered that someone spliced their cable network with a coaxial splicer.[8] At deposition, DFC's expert Shawn Kasal admitted that one can wiretap someone's internet connection with a coaxial cable splicer, and spoke of his knowledge of military wire-tapping surveillance techniques.[9] Furthermore, when questioned about Defendant

---

[4] *See* BATES#: GUERRA 000062-87 (DFC Phase I Report (attached as Ex. B)).

[5] *See* Dep. of Dr. Guerra 45:16-46:3 (admitting she took a copy of DFC's Phase I report to the San Antonio Police Department (attached as Ex. C)).

[6] *See e.g.* BATES#: GUERRA 000340 (discussing URL tracking links deployed against Plaintiffs (marked confidential and subject to Protective Order, Ex. D available for *in camera* review)).

[7] *See* BATES#: D 000110-13 (phishing links sent to Plaintiffs by Dr. Guerra using fake email addresses) (attached as Ex. E)).

[8] *See e.g.* MCantuProd00193-206 (service appointment scheduling and billing from Spectrum Cable to identify the issue with Plaintiff's internet network, and photos of cable splicing (attached as Ex. F).

[9] *See* Dep. of S. Kasal (Jul 18, 2022) at 6:10-12:10. (discussing knowledge of military-grade splicing techniques, discussing methods of splicing, and evading further answers (attached as Ex. G)).

DFC's use of a coaxial wiretap in this case, he became evasive and refused to answer questions, citing his obligations of secrecy to the military.[10]

On September 4, 2018, Defendant Dr. Guerra took the Phase I report to the San Antonio Police Department and filed a false police report against Plaintiff Melody Joy Cantu.[11] On December 21, 2018, Plaintiff Melody Joy Cantu was arrested.[12] On June 24, 2019, all charges against Plaintiff Melody Joy Cantu were dismissed by the court. [13]

Legal Standard

Summary judgment is appropriate if the record shows that "there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law."[14] The party seeking summary judgment has the initial burden to show the absence of a material fact.[15] A genuine issue of material fact exists "if the evidence is such that a reasonable jury could return a verdict for the non-moving party."[16]

---

[10] *See* Ex. G, at 8:4-9:8 (refusing to answer questions, citing his obligation to the military).

[11] *See* GUERRA 000957-61 (police affidavit memorializing Dr. Guerra stating she hired DFC (attached as Ex. H)); Ex. B, at GUERRA 000086-87 (affidavit template provided by DFC to Dr. Guerra); Ex. D, at 45:16-46:3 (stating she took a copy of DFC's Phase I report to the San Antonio Police Department).

[12] *See* BATES#: GUERRA 000952 (docket for Plaintiff Melody Joy Cantu's criminal case in Bexar County (attached as Ex. K)); Ex. H, at GUERRA 000960-61 (bond report for Bexar County Criminal Case against Plaintiff Melody Joy Cantu); DrCantuProd#000029-30 (surety bond for criminal matter (attached as Ex. L)).

[13] *See* BATES#: GUERRA 000953-55 (order granting dismissal of criminal case against Plaintiff Melody Joy Cantu (attached as Ex. M).

[14] Fed. R. Civ. P. 56(c); *see also Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247-48 (1986).

[15] *Celotex Corp. v. Catrett*, 477 U.S. 317, 325 (1986).

[16] *Anderson*, 477 U.S. at 248.

Once a motion for summary judgment is properly made and supported, the opposing party has the burden of showing that a genuine dispute exists.[17] Thus, to defeat a properly supported motion for summary judgment, the non-moving party "must set forth specific facts showing that there is a genuine issue for trial."[18] Whether a fact is considered to be "material" is determined by the substantive law, and "[o]nly disputes over facts that might affect the outcome of the suit under the governing law will properly preclude the entry of summary judgment."[19] The facts shall be viewed, and all reasonable inferences drawn, in the light most favorable to the non-moving party.[20] Neither conclusory allegations nor unsubstantiated assertions will satisfy the nonmovant's burden."[21]

"Courts agree that a willful or intentional destruction of evidence to prevent its use in litigation can justify severe sanctions."[22] "Sanctions for spoliation of evidence may include awarding attorney fees, deeming certain facts admitted, giving an adverse inference instruction to the jury, excluding evidence or expert testimony, striking pleadings, entering a default judgment, and dismissing the case entirely."[23] Spoliation of evidence may also subject a party to criminal

---

[17] *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586-87 (1986).

[18] *Anderson*, 477 U.S. at 247-48 ("[T]he mere existence of some alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment; the requirement is that there be no genuine issue of material fact.").

[19] *Id.* at 248.

[20] *Id.* at 255.

[21] *Wallace v. Tex. Tech Univ.*, 80 F.3d 1042, 1047 (5th Cir. 1996) (quotation marks and citations omitted).

[22] *See Rimkus Consulting Grp., Inc. v. Cammarata*, 688 F. Supp. 2d 598, 618 (S.D. Tex. 2010).

[23] *Allstate Texas Lloyd's v. McKinney*, 964 F. Supp. 2d 678, 683 (S.D. Tex. 2013) (quotation marks and citation omitted).

penalties, contempt sanctions, and disciplinary sanctions.[24] Much like criminal sentencing, an appropriate discovery sanction will take into account principles of deterrence, restitution, and punishment in proportion to the significance of the violation.[25]

Argument

The discovery establishes that Dr. Guerra and DFC conspired to hack, surveil and maliciously prosecute Plaintiffs. This is not a family dispute. This is the result of Dr. Guerra's inability to move beyond the family dispute and end her personal vendetta against Plaintiffs. Dr. Guerra's Motion for Summary Judgment fails to establish that there are no genuine issues of material fact. It is clear from the record that a reasonable jury could return a verdict in favor of Plaintiffs on each of the issues brought up by Dr. Guerra in her Motion for Summary Judgment. Particularly given how both Defendants have withheld discovery related to their hacking and surveillance of Plaintiffs, as detailed in Plaintiffs' Motions to Compel. Finally, Defendant Dr. Guerra misconstrues Plaintiffs' CFAA claims by only citing one part of the statute and ignoring Plaintiffs' claims under 18 USC §1030(a)(2)(C). This Court should deny Defendant Dr. Guerra's Motion to Dismiss in its entirety.

1. Defendants Violated the CFAA

A. <u>There is Competent Summary Judgment Evidence that Dr. Guerra Accessed Plaintiff's Computers Causing Damage and Loss</u>

---

[24] *Wallace v. Ford Motor Co.*, No. 3:11-CV-567-CWR-FKB, 2013 WL 3288435, at *5 n.1 (S.D. Miss. June 28, 2013).

[25] *McKinney*, 964 F. Supp. 2d at 682-83.

Defendants are mistaken that 18 USC §1030(a)(5)(A) is the only CFAA provision at issue here. Whereas 18 USC §1030(a)(5)(A) prohibits unauthorized intentional damage to a computer, subsections B and C outline alternative theories of liability.[26] 18 USC §1030(a)(5)(B) prohibits the intentional access to a protected computer without authorization, and as a result of such conduct, recklessly causing damage.[27] 18 USC §1030(a)(5)(C) prohibits intentional unauthorized access to a computer and, and as a result of such conduct, causing damage and loss.[28] These are lower thresholds for liability that were not even addressed in Defendant's Motion for Summary Judgment.

Moreover, 18 USC §1030(a)(2)(C) has no damage requirement at all, and merely requires unauthorized access to a computer - like Plaintiff Melody Joy Cantu's smartphone and obtaining information. Precisely what Dr. Guerra did when she phished Plaintiffs with the tracking URLs provided to her by DFC.[29] The record indicates that Dr. Guerra acted with the requisite knowledge and intent to give rise to liability under the CFAA.

Dr. Guerra purposely hacked, surveilled and damaged Plaintiff's computer networks in collusion with DFC. The record shows that Dr. Guerra conspired with DFC beginning May 25, 2018. Together the Defendants planned and executed a conspiracy to purposely deploy phishing

---

[26] *See* 18 USC §1030(a)(5)(A).

[27] *See* 18 USC §1030(a)(5)(B).

[28] *See* 18 USC §1030(a)(5)(C).

[29] *See* 18 U.S.C. § 1030(a)(2)(C).

links to gain access to Plaintiff's computers.[30] Communications from DFC to Dr. Guerra describe in detail how Dr. Guerra should structure the phishing emails so that the Plaintiffs would be more inclined to click on them.[31] On August 21, 2018, Dr. Guerra intentionally followed DFC's guidance and used fake emails to send phishing links to the Plaintiffs.[32] After successfully deploying the phishing links against Plaintiffs, Dr. Guerra forwarded the phishing emails to DFC, in a display of purpose and intent.[33] This phishing violates 18 USC §1030(a)(2)(C) as well as Texas state computer law. Once Dr. Guerra acquires access to Plaintiffs' computer network, she worked with DFC to infiltrate Plaintiffs' computer networks, impairing the integrity and availability of the data on that network in violation of 18 USC §1030(a)(5)(A), 18 USC §1030(a)(5)(B) and 18 USC §1030(a)(5)(C). Both DFC and Dr. Guerra have willfully withheld discovery related to the computer intrusions, as was revealed in

---

[30] *See* Ex. H, at D 000110-D 000113 (emails in which Dr. Sandra forwards to DFC emails from fake email addresses she phished Plaintiffs with by sending URL tracking links); GUERRA 00339-46 (instructions from DFC directing Dr. Guerra how to deploy phishing links (attached as Ex. O)); Ex. B, at GUERRA 000081 (DFC Phase I report to Dr. Guerra with URL tracking link results), Ex. G at 24:4-24:10 (stating he reviewed code of the phishing links sent to Plaintiffs), 27:12-15 (conceding he reviewed raw text files), 30:19-24 (stating phishing links can be used to install malware on target networks), 35:6-22 (acknowledging he knows phishing is a crime), 37:1-7 (admitting phishing techniques employ deceptive tactics).

[31] See Ex. O, GUERRA 00339-46 (instructions from DFC directing Dr. Guerra how to deploy phishing links); Ex. G at Depo 20:12-22:3, 35:6-22 (acknowledging he knows phishing is a crime), 37:1-7 (admitting phishing techniques employ deceptive tactics).

[32] *See* Ex. H, at D 000110-D 000113 (emails in which Dr. Sandra forwards to DFC emails from fake email addresses she phished Plaintiffs with by sending URL tracking links); GUERRA 00339-46 (instructions from DFC directing Dr. Guerra how to deploy phishing links (attached as Ex. O)); Ex. B, at GUERRA 000081 (DFC Phase I report to Dr. Guerra with URL tracking link results), Ex. G at 24:4-24:10 (stating he reviewed code of the phishing links sent to Plaintiffs), 27:12-15 (conceding he reviewed raw text files), 30:19-24 (stating phishing links can be used to install malware on target networks), 35:6-22 (acknowledging he knows phishing is a crime), 37:1-7 (admitting phishing techniques employ deceptive tactics).

[33] *See e.g.* BATES#: GUERRA 000340 (discussing URL tracking links deployed against Plaintiffs (marked confidential and subject to Protective Order, Ex. D available for *in camera* review)).

depositions and by their belated piecemeal productions which indicate there is missing discovery.

The fact that both Defendants withheld discovery related to their activities is evidence the Court can consider against Defendants. DFC's Depositions revealed a host of information that DFC willfully withheld - including client management files, communications with Dr. Guerra, the existence of a server used to conduct surveillance of Plaintiffs, server logs, the existence of notes on a DFC server, only some of which has been belatedly produced to date. Dr. Guerra only produced her communications with DFC after denying at deposition that she had any, after saying she'd done a diligent search.[34] The next day emails between Dr. Guerra and DFC were produced. A reasonable jury can interpret Defendant's stonewalling on discovery as evidence of their guilt.

Once Plaintiffs' network was compromised, Dr. Guerra and DFC had free access to surveil the Plaintiffs. The connection established by DFC and Dr. Guerra damaged Plaintiffs' computer network. The threshold for damage under the CFAA is minimal and only requires any impairment to the integrity or availability of the data. Computer intrusions by their nature compromise the integrity of their data. A network disruption caused by surveillance software

[34] *See* Ex. C, at 7:5-9:15 (claiming she does not recall emailing with DFC, that she had searched responsive communications, and that she found none).

constitutes impairment to the availability of data. This necessitated Plaintiff's hiring of computer experts to deal with the network intrusion.[35]

Dr. Guerra's attack on Plaintiffs' computer networks with DFC was part of a broader campaign against Plaintiffs Melody Joy Cantu and Dr. Rodrigo Cantu. On May 25, 2018, the same day she signed a retainer with DFC, Dr. Guerra hired detective.com to investigate Plaintiffs.

Defendant Dr. Guerra incorrectly claims in her Motion for Summary Judgment that Spectrum Cable installed the wire splicer found on Plaintiffs' internet cable running to their home. Spectrum actually determined that the cable splitter was not installed by them and removed it.[36] DFC's first expert witness Shawn Kasal demonstrated knowledge of coaxial wiretapping and confirmed that coaxial cable splitters such as the one connected to Plaintiffs' network can be used to monitor the network.[37]

Defendant Dr. Guerra contends that Plaintiff Dr. Cantu's personal information was never compromised but references a section of Dr. Rodrigo Cantu's deposition in which he was asked whether he had any evidence that his personal information and passwords were obtained by DFC and Dr. Guerra. Discovery materials produced subsequent to Dr. Cantu's deposition (but

---

[35] *See* BATES#: Dr.CantuProd#000001-28 (receipts and invoices from Exhibit A Computer Forensics Investigation LLC to discover and assess damage to computer network (attached as Ex. P)), 000050-51 (invoices from Exhibit A Computer Forensics Investigation LLC for consultation services provided (attached as Ex. Q))

[36] *See e.g.* MCantuProd00193-206 (service appointment scheduling and billing from Spectrum Cable to identify the issue with Plaintiff's internet network, and photos of cable splicing (attached as Ex. F).

[37] *See* Dep. of S. Kasal (Jul 18, 2022) at 6:10-12:10. (discussing knowledge of military-grade splicing techniques, discussing methods of splicing, and evading further answers (attached as Ex. G)).

requested by Plaintiffs before) reveal that DFC had compiled a report on Dr. Cantu that included his personal information, including his Dr. Cantu's complete Social Security number, which was later found for sale on the dark web.[38]

Defendant complains that Plaintiffs' expert Jeff Fischbach produced no expert report. That's because Defendants' deficient production prevented him from having anything to review; assuming Defendants fully produce the digital evidence they've been withholding, or belatedly producing piecemeal, then Mr. Fischbach will be able to generate a report as necessary. But Dr. Guerra cannot complain of not receiving an expert report when Defendants worked jointly to thwart Mr. Fischbach from being able to produce one.

Accordingly, this Court should deny Defendant Dr. Guerra's Motion for Summary Judgment as to the first 8 causes of action brought against her. For each of the material facts brought forth by Defendant Dr. Guerra, there is specific admissible evidence in the record indicating that there is a genuine dispute of material fact.

B. <u>There is Competent Summary Judgment Evidence that Defendants Caused over $5000 in CFAA Loss</u>

Defendant Dr. Guerra confuses CFAA damages with CFAA loss in her Motion for Summary Judgment. Damages under the CFAA have nothing to do with monetary loss and are specifically defined in nonmonetary terms. 18 USC §1030(e)(8) defines "damage" as "any

---

[38] *See* BATES#: D 000031-32 (communications between Dr. Guerra and DFC including Plaintiff Dr. Cantu's PII (marked confidential and subject to Protective Order, Ex. N available for *in camera* review); Ex. N, at D 000034-54 (DFC sends background check on Plaintiff Melody Joy Cantu to Dr. Guerra); Ex. A, at D 000060-61 (Retainer agreement between Dr. Guerra and DFC).

impairment to the integrity or availability of data, a program, a system, or information.[39] 18 USC §1030(e)(11) defines "loss" as any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[40] Moreover, Defendant relies on outdated caselaw when discussing CFAA damages, as the statute was amended in 2001 to separately define the loss and damage provisions.

The discovery evidences that Defendants have caused well over $5000.00 in losses as a direct result of their unauthorized access and damage to Plaintiff's computers and systems. Attached are receipts documenting Plaintiffs' losses totaling $23,650.31.[41]

Plaintiffs' CFAA loss falls into two categories. The first set of loss arises from the measures Plaintiffs took to investigate and mitigate Defendants' computer intrusions. These costs included hiring Exhibit A Computer Forensic Investigations, LLC, a computer consulting firm, to analyze their networks.[42] The retainer alone to hire the computer consultant company was $5000.00, a sufficient total to warrant liability under the CFAA.[43] This category of loss also

---

[39] *See* 18 USC §1030(e)(8).

[40] *See* 18 USC §1030(e)(11).

[41] *See* Ex. P (billing records for computer consultant, Exhibit A Computer Forensic Investigations, LLC); Ex. F (billing records from Spectrum Cable); and Ex. S (billing records for medical providers).

[42] *See* Ex. P at Dr.CantuProd#000001, 000003, 000005-14, 000016-000019 (Computer Forensic Investigations, LLC retainer and billing records).

[43] *See* Ex. P at Dr.CantuProd#000005 (retainer agreement signed with Computer Forensic Investigations, LLC).

includes the costs associated with having Spectrum Cable come out to the property to analyze, test and fix the computer networks that were unlawfully damaged by Defendants.[44] Defendants conduct necessitated that Plaintiffs schedule multiple visits from Spectrum Cable to figure out what was going on with their network, as well as a Spectrum Cable upgrade.[45] The sum total of this category of cost is $14,565.31.[46] This is well over the required CFAA loss threshold.

The second category of loss stems from the counselling and therapy necessitated by Defendants campaign of stalking and harassment of which their computer hacking and malicious prosecution was part. Defendants' computer intrusion was an integral component of their malicious prosecution. Defendants' unlawful access and damage to Plaintiffs' protected computers inflicted significant emotional stress. Related medical expenses are ongoing and currently total $9,085.00, excluding costs of prescribed medications.[47] Plaintiffs have visited Dr. John Seals, costing a total of $1,940.00[48]; Dr. Randy Pollock costing $6,945.00[49]; and Dr. Joann Murphy costing $200.00[50]. These costs continue to mount as Plaintiffs work through the psychological trauma suffered as a direct result of Defendants unlawful access and damage to

---

[44] *See e.g.* Ex. F, at MCantuProd00193-199 (service appointment scheduling and billing from Spectrum Cable to identify the issue with Plaintiff's internet network, and photos of cable splicing).

[45] *See e.g.* Ex. F at MCantuProd00193-206 (service appointment scheduling and billing from Spectrum Cable to identify the issue with Plaintiff's internet network, and photos of cable splicing)

[46] *See* Ex. P at Dr.CantuProd#000001; 000003; 000006-07.

[47] *See* MCantuFinalProd#Bates 000796-828, 001619-001679 (Medical Billing Records (attached as Ex. S)).

[48] *See* Ex. S, at 000799-000800 (Billing records from Dr. John Seals)

[49] *See* Ex. S, at 000805-000828 (Billing records from Dr. Randy Pollock)

[50] *See* Ex. S, at 000796-000798 (Billing records from Dr. Joann Murphy)

Plaintiffs' networks and protected computers. Plaintiff received detailed doctor's notes from their healthcare providers.[51]

2. Defendants violated Texas's Harmful Access by a Computer Act

For the same reasons stated above, the record establishes that Defendants acted with knowledge and intent and violated Texas's Harmful Access by a Computer Act. Dr. Guerra knowingly sent Plaintiffs phishing links, in violation of Texas criminal law. DFC guided Dr. Guerra on accessing Plaintiffs' networks.[52] Having established access, Dr. Guerra and DFC knowingly acted with intent to obtain information from, and damage, Plaintiffs' computer network.

3. Defendants violated the Federal Wire Tap Act

Dr. Guerra is incorrect that Plaintiffs alleged she installed the cable splitter. However, Dr. Guerra hired DFC and DFC's expert Shawn Kasal demonstrated a high level of knowledge of coaxial wiretapping technique, including military wiretapping applications.[53] A reasonable jury could find that Defendants violated Federal Wiretap law by splicing into Plaintiffs' network. As

---

[51] *See* MCantuPRod#Bates 000829-000848; 001512-001615, 001619-1679 (Doctor's notes (attached as Ex. T)).

[52] *See* Ex. H, at D 000110-D 000113 (emails in which Dr. Sandra forwards to DFC emails from fake email addresses she phished Plaintiffs with by sending URL tracking links); GUERRA 00339-46 (instructions from DFC directing Dr. Guerra how to deploy phishing links (attached as Ex. O)); Ex. B, at GUERRA 000081 (DFC Phase I report to Dr. Guerra with URL tracking link results), Ex. G at 24:4-24:10 (stating he reviewed code of the phishing links sent to Plaintiffs), 27:12-15 (conceding he reviewed raw text files), 30:19-24 (stating phishing links can be used to install malware on target networks), 35:6-22 (acknowledging he knows phishing is a crime), 37:1-7 (admitting phishing techniques employ deceptive tactics).

[53] *See* Ex. G at 6:10-12:10. (discussing knowledge of military-grade splicing techniques, discussing methods of splicing, and evading further answers).

mentioned above, Spectrum Cable visited Plaintiffs' home in-person and discovered that the cable splitter was not installed by anyone from their company.

4. There is no Collateral Estoppel

Defendant mistakenly claims that the intentional infliction of emotion distress here is related to a custody enforcement settlement in Bexar County District Court which she claims collaterally estops Plaintiffs' IIED claims. However, Plaintiffs' IIED claims, as pleaded in the Amended Complaint, are a direct result of Defendants' malicious campaign of stalking, hacking, and surveilling towards the ultimate goal of the malicious prosecution of Plaintiff Melody Joy Cantu. They are not based on the mediated settlement order and Defendants cannot avoid her liability for their malicious hacking and prosecution of Plaintiffs by trying to pretend that this is merely a domestic dispute.

Conclusion

For the reasons stated above, this Court should deny Defendant Dr. Guerra's Motion for Summary Judgment and deny Dr. Guerra any further relief sought.

Los Angeles, CA
Dated: October 27, 2022

Respectfully submitted,

/s/ Michael Hassard
(NY Bar No. 5824768)
Tor Ekeland Law, PLLC
30 Wall Street, 8th Floor
New York, NY
(718) 737 - 7264
michael@torekeland.com

/s/ Tor Ekeland
(NY Bar No. 4493631)
Pro Hac Vice
Tor Ekeland Law, PLLC
30 Wall Street, 8th Floor
New York, NY
(718) 737 - 7264
tor@torekeland.com

Counsel for Plaintiffs Melody Joy Cantu and Dr. Rodrigo Cantu

Certificate of Service

I certify that on this 27th of October 2022, a true and correct copy of the foregoing was electronically filed with the Clerk of the Court using the CM/ECF system which will send electronic notification of such filing to the parties on record.

/s/ Michael Hassard